

COMPLETE TRANSITIVITY OF THE NORDSTROM-ROBINSON CODES.

NEIL I. GILLESPIE AND CHERYL E. PRAEGER

ABSTRACT. In his doctorate thesis, Snover proved that any binary $(m, 256, \delta)$ code is equivalent to the Nordstrom-Robinson code or the punctured Nordstrom-Robinson code for $(m, \delta) = (16, 6)$ or $(15, 6)$ respectively. By replacing the condition that the code consists of 256 codewords with the requirement that the code is *completely regular*, we prove that the same result holds. Moreover, we prove that these codes are *completely transitive*.

1. INTRODUCTION

Snover [17] proved that any binary $(16, 256, 6)$ code is equivalent to the Nordstrom-Robinson code, and similarly that any binary $(15, 256, 5)$ code is equivalent to the punctured Nordstrom-Robinson code. The Nordstrom-Robinson codes are interesting as they are the largest possible binary codes with their length and minimum distance, and twice as large as any binary linear codes with the same length and minimum distance [16]. In this paper, we prove that the Nordstrom-Robinson codes are *completely transitive*, and hence *completely regular* (see Definition 2.2). Additionally we prove these completely regular codes are determined up to equivalence by their length and minimum distance.

Theorem 1.1. *Let C be a binary completely regular code of length m with minimum distance δ .*

- (a) *If $(m, \delta) = (16, 6)$, then C is equivalent to the Nordstrom-Robinson code;*
- (b) *If $(m, \delta) = (15, 5)$, then C is equivalent to the punctured Nordstrom-Robinson code.*

Moreover, the codes C in (a) and (b) are completely transitive.

Remark 1.2. It is known that completely transitive codes are necessarily completely regular [13]. A consequence of Theorem 1.1 is that the converse holds for binary codes with $(m, \delta) = (16, 6)$ or $(15, 5)$. This is similar to a result in [11] in which the authors proved that a binary completely regular code with $(m, \delta) = (12, 6)$ or $(11, 5)$ is unique up to equivalence, and that such codes are completely transitive.

Date: draft typeset March 4, 2013

2000 Mathematics Subject Classification: 20B25, 94B05, 05C25.

Key words and phrases: Nordstrom-Robinson codes, completely transitive codes, completely regular codes, automorphism groups

This research was supported by the Australian Research Council Federation Fellowship FF0776186 of the second author.

In Section 2, we introduce the necessary definitions and preliminary results. Then in Section 3, we prove that the Nordstrom-Robinson codes are completely transitive. In the final section we prove Theorem 1.1.

2. DEFINITIONS AND PRELIMINARIES

The *binary Hamming graph* Γ_m is the graph with vertex set, $V(\Gamma_m)$, equal to the set of m -tuples with entries from the field $\mathbb{F}_2 = \{0, 1\}$, and an edge exists between two vertices if and only if they differ in precisely one entry. Any binary code of length m can be embedded as a subset of $V(\Gamma_m)$. The automorphism group of Γ_m , which we denote by $\text{Aut}(\Gamma_m)$, is the semi-direct product $\mathfrak{B} \rtimes \mathfrak{L}$ where $\mathfrak{B} \cong S_2^m$ and $\mathfrak{L} \cong S_m$, see [5, Theorem 9.2.1]. Let $g = (g_1, \dots, g_m) \in \mathfrak{B}$, $\sigma \in \mathfrak{L}$ and $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma_m)$. Then $g\sigma$ acts on α in the following way:

$$\alpha^{g\sigma} = (\alpha_{1\sigma^{-1}}^{g_{1\sigma^{-1}}}, \dots, \alpha_{m\sigma^{-1}}^{g_{m\sigma^{-1}}}).$$

We can view $V(\Gamma_m)$ as the vector space \mathbb{F}_2^m of m -dimensional row vectors over \mathbb{F}_2 . Furthermore, because the base group $\mathfrak{B} \cong S_2^m$ of $\text{Aut}(\Gamma_m)$ is regular on $V(\Gamma_m)$, we may identify \mathfrak{B} with the group of translations of \mathbb{F}_2^m , and $\text{Aut}(\Gamma_m)$ with a subgroup of the affine group $\text{AGL}(m, 2)$. More precisely \mathfrak{B} consists of the translations g_α , where $\beta^{g_\alpha} = \beta + \alpha$ for $\alpha, \beta \in \mathbb{F}_2^m$, and if $\mathbf{0}$ is the zero vector, then $\text{Aut}(\Gamma_m) = \mathfrak{B} \rtimes \text{Aut}(\Gamma_m)_{\mathbf{0}}$ where $\text{Aut}(\Gamma_m)_{\mathbf{0}}$ (the stabiliser of $\mathbf{0}$ in $\text{Aut}(\Gamma_m)$) is the group of permutation matrices in $\text{GL}(m, 2)$.

Let $M = \{1, \dots, m\}$, and view M as the set of vertex entries of Γ_m . For $\alpha \in \mathbb{F}_2^m$, the *support* of α is the set $\text{supp}(\alpha) = \{i \in M : \alpha_i \neq 0\}$, and the *weight* of α is $\text{wt}(\alpha) = |\text{supp}(\alpha)|$. We let α^c denote the unique vertex in \mathbb{F}_2^m such that $\text{supp}(\alpha^c) = M \setminus \text{supp}(\alpha)$. For all pairs of vertices $\alpha, \beta \in \mathbb{F}_2^m$, the *Hamming distance* between α and β , denoted by $d(\alpha, \beta)$, is defined to be the number of entries in which the two vertices differ. We let $\Gamma_{m,k}(\alpha)$ denote the set of vertices in Γ_m that are at distance k from α .

Let C be a code in Γ_m . The *minimum distance*, δ , of C is the smallest distance between distinct codewords of C . If C is a subspace of \mathbb{F}_2^m with dimension k , we say C is a *linear* $[m, k, \delta]$ code. If C is not a linear code we say C is a $(m, |C|, \delta)$ code, where $|C|$ denotes the cardinality of C . For any vertex $\gamma \in \mathbb{F}_2^m$, we define the *distance of γ from C* to be $d(\gamma, C) = \min\{d(\gamma, \beta) \mid \beta \in C\}$. The *covering radius* of C is the maximum distance any vertex in \mathbb{F}_2^m is from C . We let C_i denote the set of vertices that are distance i from C . It follows that $\{C = C_0, C_1, \dots, C_\rho\}$ forms a partition of \mathbb{F}_2^m , called the *distance partition* of C . The *distance distribution* of C is the $(m+1)$ -tuple $a(C) = (a_0, \dots, a_m)$ where

$$a_i = \frac{|\{(\alpha, \beta) \in C^2 : d(\alpha, \beta) = i\}|}{|C|}.$$

We observe that $a_i \geq 0$ for all i and $a_0 = 1$. Moreover, $a_i = 0$ for $1 \leq i \leq \delta - 1$ and $|C| = \sum_{i=0}^m a_i$. The *MacWilliams transform* of $a(C)$ is the $(m+1)$ -tuple $a'(C) = (a'_0, \dots, a'_m)$ where

$$(1) \quad a'_k := \sum_{i=0}^m a_i K_k(i)$$

with

$$K_k(x) := \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{m-x}{k-j}.$$

It follows from [15, Lemma 5.3.3] that $a'_k \geq 0$ for $k \in \{0, 1, \dots, m\}$. We define the *automorphism group of C* to be the setwise stabiliser of C in $\text{Aut}(\Gamma_m)$, which we denote by $\text{Aut}(C)$. We let $\text{Perm}(C)$ denote the group of permutation matrices that fix C setwise. We also note that $\text{Aut}(C)$ preserves the distance partition of C [12, Lemma 2.6].

Remark 2.1. In traditional coding theory, only weight preserving automorphisms of a code are considered, and so in the binary case, $\text{Perm}(C)$ is defined as the automorphism group of a code. Consequently, established results about automorphism groups of certain codes refer to $\text{Perm}(C)$, not $\text{Aut}(C)$. However, if $\mathbf{0} \in C$ we note that $\text{Aut}(C)_{\mathbf{0}}$ is equal to $\text{Perm}(C)$.

We say two codes C and C' in Γ_m are *equivalent* if there exists $x \in \text{Aut}(\Gamma_m)$ such that $C^x = C'$.

Definition 2.2. Let C be code in Γ_m with distance partition $\{C, C_1, \dots, C_\rho\}$ and $\gamma \in C_i$. We say C is *completely regular* if $|\Gamma_{m,k}(\gamma) \cap C|$ depends only on i and k , and not on the choice of $\gamma \in C_i$. If there exists $X \leq \text{Aut}(\Gamma_m)$ such that each C_i is an X -orbit, then we say C is *X -completely transitive*, or simply *completely transitive*.

A code C in Γ_m is *antipodal* if $\alpha^c \in C$ for all $\alpha \in C$, otherwise we say C is *non-antipodal*. The following result is straight forward to prove.

Lemma 2.3. *Let C be an antipodal code in Γ_m with distance distribution $a(C) = (a_0, \dots, a_m)$. Then $a_i = a_{m-i}$ for $0 \leq i \leq m$.*

Borges et al. [3] classified all binary, non-antipodal completely regular codes containing more than two codewords. The following is a consequence of their classification.

Proposition 2.4. *Let C be a completely regular code in Γ_m with $\delta \geq 5$ and $|C| > 2$. If $m \neq 22$ or 23 , then C is antipodal.*

Let $p \in M = \{1, \dots, m\}$ and C be a code in Γ_m . By deleting the same coordinate p from each codeword of C , we generate a code in Γ_{m-1} , which we call the *punctured code of C with respect to p* . We can also describe this code in the following way. Let $J = \{i_1, \dots, i_k\} \subseteq M$ and define the following map

$$\begin{aligned} \pi_J : \quad \mathbb{F}_2^m &\longrightarrow \mathbb{F}_2^{|J|} \\ (\alpha_1, \dots, \alpha_m) &\longmapsto (\alpha_{i_1}, \dots, \alpha_{i_k}) \end{aligned}$$

We define the *projected code of C with respect to J* to be the set $\pi_J(C) = \{\pi_J(\alpha) : \alpha \in C\}$. It follows that if $J = M \setminus \{p\}$ then $\pi_J(C)$ is equal to the punctured code of C with respect to p . When we project we would like to have some group information available to us. We have an induced action of $\text{Aut}(\Gamma_m)_J = \{g \in \text{Aut}(\Gamma_m) : J^g = J\}$ as follows: for $x \in \text{Aut}(\Gamma_m)_J$, we define

$$(2) \quad \begin{aligned} \chi(x) : \quad \mathbb{F}_2^{|J|} &\longrightarrow \mathbb{F}_2^{|J|} \\ \pi_J(\alpha) &\longmapsto \pi_J(\alpha^x), \end{aligned}$$

and observe that $\ker \chi = \{(g_1, \dots, g_m)\sigma \in \text{Aut}(\Gamma_m)_J : j^\sigma = j \text{ and } g_j = 1 \text{ for } j \in J\}$.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ where \mathcal{P} is a set of points of cardinality m , and \mathcal{B} is a set of k subsets of \mathcal{P} called blocks. Then \mathcal{D} is a $t - (m, k, \lambda)$ design if every t -subset of \mathcal{P} is contained in exactly λ blocks of \mathcal{B} . We let b denote the number of blocks in a design. If \mathcal{D} is a t -design, then it is also an $i - (m, k, \lambda_i)$ design for $0 \leq i \leq t - 1$ [7, Corollary 1.6] where

$$(3) \quad \lambda_i \binom{k-i}{t-i} = \lambda \binom{m-i}{t-i}.$$

Using this fact we can deduce that

$$(4) \quad \binom{m}{i} \lambda_i = b \binom{k}{i}.$$

For further concepts and definitions about t -designs see [7]. There is an analogous concept of t -designs for subsets of vertices in \mathbb{F}_2^m . Let α, β be two vertices in \mathbb{F}_2^m . Then we say α is *covered* by β if for each non-zero component α_i of α it holds that $\alpha_i = \beta_i$.

Definition 2.5. Let \mathcal{D} be a set of vertices of weight k in Γ_m . Then we say \mathcal{D} is a *2-ary t -(m, k, λ) design* if for every vertex ν of weight t , there exist exactly λ vertices of \mathcal{D} that cover ν .

This definition coincides with the usual definition of a t -design, in the sense that the set of blocks is the set of supports of vertices in \mathcal{D} . Therefore, when we consider 2-ary t -designs in Γ_m , we simply refer to them as t -designs. The following is a consequence of a result proved by Van Tilborg [18, Theorem 2.4.7]. For a code C and a positive integer k we denote by $C(k)$ the set of weight k codewords of C .

Theorem 2.6. *Let C be a completely regular code in Γ_m that contains the zero vertex. Then for each k with $\delta \leq k \leq m$ and $C(k) \neq \emptyset$, it holds that $C(k)$ forms a 2-ary t -design with $t = \lfloor \frac{\delta}{2} \rfloor$.*

2.1. The Nordstrom-Robinson code \mathcal{N} . We give the description of the Nordstrom-Robinson code \mathcal{N} due to Goethals [14]. It is a code in Γ_{16} constructed from the extended binary Golay code \mathcal{G} in Γ_{24} (as defined, for example, in [7, p.131]). This requires *concatenation notation*. For any $\bar{\alpha} \in \mathbb{F}_2^{24}$, we can write $\bar{\alpha}$ as the concatenation of a vertex in \mathbb{F}_2^8 followed by a vertex in \mathbb{F}_2^{16} . That is

$$\bar{\alpha} = (\bar{\alpha}_1, \dots, \bar{\alpha}_{24}) = \mathbf{u}\alpha,$$

where $\mathbf{u} = (\bar{\alpha}_1, \dots, \bar{\alpha}_8) \in \mathbb{F}_2^8$, $\alpha = (\bar{\alpha}_9, \dots, \bar{\alpha}_{24}) \in \mathbb{F}_2^{16}$. We note, for $\bar{\beta} = \mathbf{v}\beta \in \mathbb{F}_2^{24}$, that $\bar{\alpha} + \bar{\beta} = \mathbf{u}\alpha + \mathbf{v}\beta = (\mathbf{u} + \mathbf{v})(\alpha + \beta)$.

Let \mathcal{G} be the $[24, 12, 8]$ extended binary Golay code, chosen so that $\bar{\gamma} = (1^8, 0^{16}) \in \mathcal{G}$. It is known that $\text{Perm}(\mathcal{G}) \cong M_{24}$ [16, Ch. 20], and hence $\text{Aut}(\mathcal{G}) = T_{\mathcal{G}} \rtimes \text{Perm}(\mathcal{G})$ where $T_{\mathcal{G}}$ is the group of translations generated by \mathcal{G} [13]. Furthermore, by [9, p.96]

$$H := \text{Perm}(\mathcal{G})_{\bar{\gamma}} \cong \text{AGL}(4, 2) \cong 2^4 : A_8.$$

Let $J^* = \{1, \dots, 8\}$ and $J = M \setminus J^*$. Then H has an induced action on J^* that is permutationally isomorphic to A_8 acting on J^* , and a faithful action on J . We define the following subcode of \mathcal{G} :

$$\mathcal{C} = \{\bar{\alpha} \in \mathcal{G} : \text{supp}(\bar{\alpha}) \cap J^* = \emptyset\}.$$

Clearly \mathcal{C} is a linear subcode of \mathcal{G} , and it follows that $H \leq \text{Perm}(\mathcal{C})$. For $1 \leq i \leq 7$, let $\bar{\alpha}_i$ be a codeword in \mathcal{G} with $\text{supp}(\bar{\alpha}_i) \cap J^* = \{i, 8\}$ (such codewords exist in \mathcal{G} , see [16, p.73]), and let \mathcal{C}^i be the coset $\bar{\alpha}_i + \mathcal{C}$. It follows that \mathcal{C}^i consists of all the codewords $\bar{\alpha} \in \mathcal{G}$ such that $\text{supp}(\bar{\alpha}) \cap J^* = \{i, 8\}$. Let \mathbf{u}_0 be the zero vertex in \mathbb{F}_2^8 and for $i = 1, \dots, 7$, let $\mathbf{u}_i \in \mathbb{F}_2^8$ such that $\text{supp}(\mathbf{u}_i) = \{i, 8\}$. For $i = 0, 1, \dots, 7$ it holds that $\pi_{J^*}(\bar{\alpha}) = \mathbf{u}_i$ for all $\bar{\alpha} \in \mathcal{C}^i$, where $\mathcal{C}^0 = \mathcal{C}$.

Definition 2.7. Let $\mathcal{B} = \bigcup_{i=0}^7 \mathcal{C}^i$, where $\mathcal{C}^0 = \mathcal{C}$. The *Nordstrom-Robinson code* \mathcal{N} is defined to be the projection code of \mathcal{B} onto J . That is, $\mathcal{N} = \pi_J(\mathcal{B})$.

Let \mathcal{R} be the subcode of \mathcal{N} equal to the projection code of \mathcal{C} onto J , and for $i = 1, \dots, 7$ let \mathcal{R}^i be the projection code of \mathcal{C}^i onto J , so $\mathcal{N} = \bigcup_{i=0}^7 \mathcal{R}^i$ where $\mathcal{R} = \mathcal{R}^0$. The code \mathcal{R} is the Reed Muller code $R(1, 4)$, which is a linear $[16, 5, 8]$ code [16, p.74], and it follows, for each $i = 1, \dots, 7$, that \mathcal{R}^i is a coset of \mathcal{R} .

Berlekamp proved that \mathcal{N} is a binary $(16, 256, 6)$ code, and that $\text{Perm}(\mathcal{N}) = 2^4 : A_7$ acting 3-transitively on 16 points [2]. Therefore, by our definition of the automorphism group of a code, $\text{Aut}(\mathcal{N})_{\mathbf{0}} = 2^4 : A_7$, where $\mathbf{0}$ is the zero codeword in \mathcal{N} . Furthermore, \mathcal{N} is an *even* code, by which we mean that every codeword in \mathcal{N} has even weight [16, p.74], and the covering radius of \mathcal{N} is $\rho = 4$ [1, Corollary 5.2].

3. COMPLETE TRANSITIVITY OF THE NORDSTROM-ROBINSON CODES

Recall that $\text{Aut}(\mathcal{N})$ is the stabiliser of \mathcal{N} in $\text{Aut}(\Gamma_{16})$. The following homomorphism defines an action of $\text{Aut}(\mathcal{N})$ on $M = \{1, \dots, 16\}$.

$$(5) \quad \begin{array}{ccc} \mu : \text{Aut}(\mathcal{N}) & \longrightarrow & S_{16} \\ g\sigma & \longmapsto & \sigma \end{array}$$

Lemma 3.1. Let K be the kernel of the map μ in (5) and let \mathcal{R} be the Reed Muller code contained in \mathcal{N} . Then $K = T_{\mathcal{R}}$, the group of translations of \mathbb{F}_2^{16} generated by \mathcal{R} .

Proof. Let $g = (h_1, \dots, h_{16}) \in K$. Then there exists $\beta \in \mathbb{F}_2^{16}$ such that we can identify g with the translation g_{β} of \mathbb{F}_2^{16} . Consequently, because $g_{\beta} \in \text{Aut}(\mathcal{N})$ and $\mathbf{0} \in \mathcal{N}$, it follows that $\beta = \mathbf{0} + \beta = \mathbf{0}^{g_{\beta}} \in \mathcal{N}$. Suppose first that $\beta \in \mathcal{R}$, and let $\alpha \in \mathcal{N}$. Then $\bar{\beta} = \mathbf{u}_0\beta \in \mathcal{C}$ and there exists $i \in \{0, \dots, 7\}$ such that $\bar{\alpha} = \mathbf{u}_i\alpha \in \mathcal{C}^i$. As \mathcal{G} is a linear code, we deduce that

$$\bar{\nu} := \mathbf{u}_i\alpha + \mathbf{u}_0\beta = (\mathbf{u}_i + \mathbf{u}_0)(\alpha + \beta) = \mathbf{u}_i(\alpha + \beta) \in \mathcal{G}.$$

If $i \neq 0$ then $\text{supp}(\bar{\nu}) \cap J^* = \{i, 8\}$, and if $i = 0$ then $\text{supp}(\bar{\nu}) \cap J^* = \emptyset$. Thus $\bar{\nu} = \mathbf{u}_i(\alpha + \beta) \in \mathcal{C}^i$, and so $\alpha^{g_{\beta}} = \alpha + \beta \in \mathcal{N}$. Consequently, $T_{\mathcal{R}} \leq K$.

Now suppose that $\beta \in \mathcal{N} \setminus \mathcal{R}$. Then there exists $j \in \{1, \dots, 7\}$ such that $\bar{\beta} = \mathbf{u}_j\beta \in \mathcal{C}^j$. Let $\alpha \in \mathcal{R}^i$ where $i \notin \{0, j\}$, so $\bar{\alpha} = \mathbf{u}_i\alpha \in \mathcal{C}^i$. Since $g_{\beta} \in \text{Aut}(\mathcal{N})$ it follows that $\alpha + \beta \in \mathcal{N}$, and so there exists $k \in \{0, \dots, 7\}$ such that $\mathbf{u}_k(\alpha + \beta) \in \mathcal{C}^k$. Furthermore, as \mathcal{G} is linear, we have that

$\bar{\alpha} + \bar{\beta} = (\mathbf{u}_i + \mathbf{u}_j)(\alpha + \beta) \in \mathcal{G}$. It follows from the definitions that $\mathbf{u}_i + \mathbf{u}_j$ is a weight 2 vertex in \mathbb{F}_2^8 with non-zero entries in positions i and j . Consequently

$$d(\mathbf{u}_k(\alpha + \beta), (\mathbf{u}_i + \mathbf{u}_j)(\alpha + \beta)) = \begin{cases} 2 & \text{if } k \in \{0, i, j\} \\ 4 & \text{otherwise} \end{cases}$$

which contradicts the fact that \mathcal{G} has minimum distance 8. Hence $K = T_{\mathcal{R}}$. \square

Theorem 3.2. \mathcal{N} is $\text{Aut}(\mathcal{N})$ -completely transitive.

Proof. We first prove that for each $\beta \in \mathcal{N}$, there exists an $x \in \text{Aut}(\mathcal{N})$ such that $\beta^x = \mathbf{0}$, and hence $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N} . Let $\beta \in \mathcal{R}$ then, by Lemma 3.1, $g_{\beta} \in \text{Aut}(\mathcal{N})$, and it follows that $\beta^{g_{\beta}} = \beta + \beta = \mathbf{0}$. Now suppose that $\beta \in \mathcal{N} \setminus \mathcal{R}$. Then there exists a unique $i \in \{1, \dots, 7\}$ such that $\bar{\beta} = \mathbf{u}_i \beta \in \mathcal{C}^i = \bar{\alpha}_i + \mathcal{C}$. Let g be the translation of Γ_{24} generated by $\bar{\alpha}_i$, let $\sigma \in H$ such that $i^{\sigma} = 8$, and let $x = g\sigma \in \text{Aut}(\mathcal{G})$. We claim that $\chi(x) \in \text{Aut}(\mathcal{N})$, where χ is as in (2).

Since $\sigma \in \text{Perm}(\mathcal{C})$ it follows that $(\bar{\alpha}_i + \mathcal{C})^x = (\bar{\alpha}_i + \bar{\alpha}_i + \mathcal{C})^{\sigma} = \mathcal{C}^{\sigma} = \mathcal{C}$. In particular, $\bar{\beta}^x \in \mathcal{C}$. Furthermore, $\mathcal{C}^x = (\bar{\alpha}_i + \mathcal{C})^{\sigma} = \bar{\alpha}_i^{\sigma} + \mathcal{C}$. Now, because $\text{supp}(\bar{\alpha}_i^{\sigma}) \cap J^* = \{i^{\sigma}, 8^{\sigma}\} = \{8, 8^{\sigma}\}$ and σ stabilises J^* , it follows that $\bar{\alpha}_i^{\sigma} \in \bar{\alpha}_{8^{\sigma}} + \mathcal{C}$ and so $\mathcal{C}^x = \bar{\alpha}_{8^{\sigma}} + \mathcal{C}$. Now, for $j \neq i$ or 0, consider $\mathcal{C}^j = \bar{\alpha}_j + \mathcal{C}$. Then $(\bar{\alpha}_j + \mathcal{C})^x = (\bar{\alpha}_j + \bar{\alpha}_i + \mathcal{C})^{\sigma} = (\bar{\alpha}_j + \bar{\alpha}_i)^{\sigma} + \mathcal{C}$, because $\sigma \in \text{Perm}(\mathcal{C})$. It follows that $\text{supp}(\bar{\alpha}_j + \bar{\alpha}_i) \cap J^* = \{j, i\}$, and so $\text{supp}((\bar{\alpha}_j + \bar{\alpha}_i)^{\sigma}) \cap J^* = \{j^{\sigma}, i^{\sigma}\} = \{j^{\sigma}, 8\}$. Consequently $(\bar{\alpha}_j + \bar{\alpha}_i)^{\sigma} \in \bar{\alpha}_{j^{\sigma}} + \mathcal{C}$, and so $(\bar{\alpha}_j + \mathcal{C})^x = \bar{\alpha}_{j^{\sigma}} + \mathcal{C}$. Hence x fixes setwise \mathcal{B} . Because $\mathcal{N} = \pi_J(\mathcal{B})$ we deduce that $\chi(x) \in \text{Aut}(\mathcal{N})$.

Since $\bar{\beta}^x \in \mathcal{C}$, there exists $\eta \in \mathcal{R}$ such that $\pi_J(\bar{\beta}^x) = \eta$. By Lemma 3.1, $g_{\eta} \in K$, and so $y = \chi(x)g_{\eta} \in \text{Aut}(\mathcal{N})$, and we have, by (2),

$$\beta^y = \pi_J(\bar{\beta})^{\chi(x)g_{\eta}} = \pi_J(\bar{\beta}^x)^{g_{\eta}} = \eta^{g_{\eta}} = \eta + \eta = \mathbf{0}.$$

Consequently, $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N} .

Recall that \mathcal{N} has covering radius $\rho = 4$, and so $\{\mathcal{N}, \mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3, \mathcal{N}_4\}$ is the distance partition of \mathcal{N} . Recall that $\text{Aut}(\mathcal{N})_{\mathbf{0}} \cong 2^4 : A_7$ acting 3-transitively on 16 points. Furthermore, because \mathcal{N} has minimum distance 6, it follows that $\Gamma_{16,i}(\mathbf{0}) \subseteq \mathcal{N}_i$ for $i = 1, 2, 3$. Therefore $\text{Aut}(\mathcal{N})_{\mathbf{0}}$ acts transitively on $\Gamma_{16,i}(\mathbf{0}) = \Gamma_{16,i}(\mathbf{0}) \cap \mathcal{N}_i$, and so by [11, Lemma 2.4], $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N}_i for $i = 1, 2, 3$.

Let $\nu \in \Gamma_{16,4}(\mathbf{0})$. Then ν is the neighbour of a weight 3 vertex, which, as stated above, is an element of \mathcal{N}_3 . Therefore $\nu \in \mathcal{N}_2 \cup \mathcal{N}_3 \cup \mathcal{N}_4$. Suppose $\nu \in \mathcal{N}_3$. Then there exists $\alpha \in \mathcal{N}$ such that $d(\nu, \alpha) = 3$. As ν has weight 4, this implies that α has odd weight, which contradicts the fact that every codeword of \mathcal{N} has even weight. Thus $\nu \in \mathcal{N}_2 \cup \mathcal{N}_4$. Since $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N} , and because the distance partition of \mathcal{N} is preserved by $\text{Aut}(\mathcal{N})$, it follows that $\Gamma_{16,4}(\mathbf{0}) \cap \mathcal{N}_4 \neq \emptyset$. Also, let β be any codeword of weight 6, and let $\nu^* \in \Gamma_{16,4}(\mathbf{0})$ be such that $\text{supp}(\nu^*) \subseteq \text{supp}(\beta)$. Then $d(\nu^*, \beta) = 2$, and so $\Gamma_{16,4}(\mathbf{0}) \cap \mathcal{N}_2 \neq \emptyset$. Consequently, because $\text{Aut}(\mathcal{N})_{\mathbf{0}}$ fixes setwise $\Gamma_{16,4}(\mathbf{0})$ and preserves the distance partition of \mathcal{N} , $\text{Aut}(\mathcal{N})_{\mathbf{0}}$ has at least 2 orbits on $\Gamma_{16,4}(\mathbf{0})$. Moreover, we see in [10, Table XI] that $\text{Perm}(\mathcal{N}) = \text{Aut}(\mathcal{N})_{\mathbf{0}}$ has exactly two orbits on $\Gamma_{16,4}(\mathbf{0})$. Thus $\text{Aut}(\mathcal{N})_{\mathbf{0}}$ acts transitively on $\Gamma_{16,4}(\mathbf{0}) \cap \mathcal{N}_4$, and so, by [11, Lemma 2.4], $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N}_4 . \square

Corollary 3.3. $\text{Aut}(\mathcal{N})/K \cong 2^4 : A_8$.

Proof. Since $\text{Aut}(\mathcal{N})_{\mathbf{0}} \cap K = 1$, where K is the kernel of the map μ in (5), it follows that $\text{Aut}(\mathcal{N})_{\mathbf{0}} \cong \mu(\text{Aut}(\mathcal{N})_{\mathbf{0}})$. Recall that $\text{Aut}(\mathcal{N})_{\mathbf{0}} \cong 2^4 : A_7$, and so $\mu(\text{Aut}(\mathcal{N}))$ is a 3-transitive subgroup of S_{16} containing $2^4 : A_7$. By the classification of finite 2-transitive groups [6], it follows that $\mu(\text{Aut}(\mathcal{N})) \cong 2^4 : A_7$, $2^4 : A_8$, A_{16} or S_{16} . Because $\text{Aut}(\mathcal{N})$ acts transitively on \mathcal{N} , it holds that $|\text{Aut}(\mathcal{N})| = 2^8 \times |\text{Aut}(\mathcal{N})_{\mathbf{0}}|$. Moreover, by Lemma 3.1, $|K| = |T_{\mathcal{R}}| = 2^5$. Consequently, the only possibility is that $\mu(\text{Aut}(\mathcal{N})) \cong 2^4 : A_8$. \square

3.1. The Punctured Nordstrom-Robinson Code \mathcal{PN} . Let $p \in M = \{1, \dots, 16\}$ and $J = M \setminus \{p\}$. Recall that the punctured Nordstrom-Robinson code with respect to p is the code generated by deleting the p^{th} entry of each codeword of the Nordstrom-Robinson code \mathcal{N} . It is also equal to the projected code $\pi_J(\mathcal{N})$. By Theorem 3.2, \mathcal{N} is completely transitive, and so is completely regular. Consequently, as \mathcal{N} is an even code with covering radius equal to 4, a result by Brouwer [4] implies that $\pi_J(\mathcal{N})$ is completely regular with covering radius $\rho = 3$. Therefore, as $\mathbf{0} \in \pi_J(\mathcal{N})$, it follows that the minimum distance δ of $\pi_J(\mathcal{N})$ is equal to the minimum non-zero weight of codewords in $\pi_J(\mathcal{N})$, which is equal to either 5 or 6 as the minimum non-zero weight of codewords in \mathcal{N} is 6. By [16, p.74], $|\mathcal{N}(6)| = 112$, where $\mathcal{N}(6)$ is the set of codewords in \mathcal{N} of weight 6, and so Theorem 2.6 implies that $\mathcal{N}(6)$ forms a $3 - (16, 6, 4)$ design. Hence the number of codewords of weight 6 whose support contains p is 42, and these correspond to 42 codewords of $\pi_J(\mathcal{N})$ of weight 5. Thus $\pi_J(\mathcal{N})$ has $\delta = 5$. Consequently, $\pi_J(\mathcal{N})$ is a $(15, 256, 5)$ code. Snover [17] proved that a $(15, 256, 5)$ binary code is unique up to equivalence. Thus, for any $p' \in M$, the punctured \mathcal{N} code with respect to p' is equivalent to $\pi_J(\mathcal{N})$. Therefore, without loss of generality, we can assume that $p = 1$ as in [2], and we denote $\pi_J(\mathcal{N})$ by \mathcal{PN} . By [2, Lemma 6.5], $\text{Aut}(\mathcal{PN})_{\mathbf{0}} \cong A_7$ acting 2-transitively on 15 points. The action of $\text{Aut}(\mathcal{PN})_{\mathbf{0}} \cong A_7$ on $\Gamma_{15,3}(\mathbf{0})$ is equivalent to its action on the 3-element subsets of J . The permutation characters for the A_7 -actions on J and on the 3-element subsets of J have inner product equal to 2, see [9, p.10]. Hence A_7 has exactly two orbits on 3-element subsets of J , so $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ has exactly two orbits on $\Gamma_{15,3}(\mathbf{0})$.

Theorem 3.4. \mathcal{PN} is $\text{Aut}(\mathcal{PN})$ -completely transitive.

Proof. Let J be as above, and recall the homomorphism χ from (2) with kernel equal to $\ker \chi = \langle (g_1, \dots, g_{16}) \rangle$, where $g_p = (12)$ and $g_i = 1$ for $i \neq p$. Since $\text{Aut}(\mathcal{N}) \cap \mathfrak{B} = K = T_{\mathcal{R}}$, by Lemma 3.1, it follows that $\text{Aut}(\mathcal{N}) \cap \ker \chi = 1$. Hence $\chi(\text{Aut}(\mathcal{N})_p) \cong \text{Aut}(\mathcal{N})_p$, and it is straight forward to show that $\chi(\text{Aut}(\mathcal{N})_p) \leq \text{Aut}(\mathcal{PN})$. Also $K \leq \text{Aut}(\mathcal{N})_p$, and $\text{Aut}(\mathcal{N})/K \cong 2^4 : A_8$, by Corollary 3.3. Thus $\text{Aut}(\mathcal{N})_p/K \cong A_8$. As $\text{Aut}(\mathcal{PN})_{\mathbf{0}} \cong A_7$, it follows from the orbit stabiliser theorem that

$$|\text{Aut}(\mathcal{PN})| \leq |\mathcal{PN}| |\text{Aut}(\mathcal{PN})_{\mathbf{0}}| = |K| |A_8| = |\text{Aut}(\mathcal{N})_p|.$$

Hence, we deduce that $\text{Aut}(\mathcal{N})_p \cong \text{Aut}(\mathcal{PN})$ and $\text{Aut}(\mathcal{PN})$ acts transitively on \mathcal{PN} .

Recall that \mathcal{PN} has covering radius $\rho = 3$, and so has distance partition $\{\mathcal{PN}, \mathcal{PN}_1, \mathcal{PN}_2, \mathcal{PN}_3\}$. Since $\delta = 5$ we have that $\Gamma_{15,i}(\mathbf{0}) \subseteq \mathcal{PN}_i$ for $i = 1, 2$. Furthermore, because $\text{Aut}(\mathcal{PN})_{\mathbf{0}} \cong A_7$ acts 2-transitively on entries, it follows that $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ acts transitively on $\Gamma_{15,i}(\alpha) = \Gamma_{15,i}(\alpha) \cap \mathcal{PN}_i$

for $i = 1, 2$. Thus, by [11, Lemma 2.4], $\text{Aut}(\mathcal{PN})$ acts transitively on \mathcal{PN}_i for $i = 1, 2$. Now, let $\nu \in \Gamma_{15,3}(\mathbf{0})$. As $\delta = 5$, it follows that $\nu \in \mathcal{PN}_2 \cup \mathcal{PN}_3$. By following a similar argument to that used in the proof of Theorem 3.2, we deduce that $\Gamma_{15,3}(\mathbf{0}) \cap \mathcal{PN}_i \neq \emptyset$ for $i = 2, 3$. Thus because $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ fixes setwise $\Gamma_{15,3}(\mathbf{0})$ and preserves the distance partition of \mathcal{PN} , it follows that $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ has at least two orbits on $\Gamma_{15,3}(\mathbf{0})$. As we saw above, $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ has exactly two orbits on $\Gamma_{15,3}(\mathbf{0})$. Consequently $\text{Aut}(\mathcal{PN})_{\mathbf{0}}$ acts transitively on $\Gamma_{15,3}(\mathbf{0}) \cap \mathcal{PN}_3$. Hence, by [11, Lemma 2.4], $\text{Aut}(\mathcal{PN})$ acts transitively on \mathcal{PN}_3 . \square

4. PROOF OF THEOREM 1.1

Let C be a completely regular code in Γ_m with minimum distance δ for $(m, \delta) = (16, 6)$ or $(15, 5)$. Complete regularity and minimum distance are preserved by equivalence, therefore, by replacing C with an equivalent code if necessary, we can assume that $\mathbf{0} \in C$. Since C contains $\mathbf{0}$ and is completely regular, it follows that $C(\delta) \neq \emptyset$, where $C(\delta)$ is the set of codewords of weight δ . Hence, by Theorem 2.6, $C(\delta)$ forms a $t - (m, \delta, \lambda)$ design for $t = \lfloor \frac{\delta}{2} \rfloor$ and some positive integer λ . We deduce (in both cases $(m, \delta) = (16, 6)$ or $(15, 5)$), using (3) and (4), that 2 divides λ . Let S be the set of $\alpha \in C(\delta)$ such that $\{1, \dots, t\} \subset \text{supp}(\alpha)$. It follows that $|S| = \lambda$, and as C has minimum distance δ , we deduce that $\text{supp}(\alpha) \cap \text{supp}(\beta) = \{1, \dots, t\}$ for all distinct pairs of codewords $\alpha, \beta \in S$. Consequently, a simple counting argument gives that

$$\lambda \leq \frac{m-t}{\delta-t}.$$

In both cases we deduce that $\lambda < 5$, so $\lambda = 2$ or 4 . However, by Line 21 of [8, Table 3.37] and Line 16 of [8, Table 1.28], it follows that a $t - (m, \delta, \lambda)$ design does not exist in both cases for $\lambda = 2$. Thus $\lambda = 4$. Consequently $|C| > 2$ in both cases, and so, by Proposition 2.4, we have that C is antipodal. Therefore, if $a(C) = (a_0, \dots, a_m)$, we deduce, by Lemma 2.3, that $a_i = a_{m-i}$ for all i .

Case $(m, \delta) = (16, 6)$: In this case $C(6)$ forms a $3 - (16, 6, 4)$ design, and so $|C(6)| = 112$. It then follows, because C is antipodal, that

$$a(C) = (1, 0, 0, 0, 0, 0, 112, a_7, a_8, a_7, 112, 0, 0, 0, 0, 0, 1).$$

It follows from (1) and [15, Lemma 5.3.3] that the following constraints must hold:

$$\begin{aligned} 240 - 12a_7 - 8a_8 &\geq 0 \\ -840 - 28a_7 + 28a_8 &\geq 0 \end{aligned}$$

with $a_7 \geq 0$ and $a_8 \geq 0$. Solving these constraints gives that $a_7 = 0$ and $a_8 = 30$. Consequently C is a $(16, 256, 6)$ binary code, and so, by Snover's result [17], C is equivalent to the Nordstrom-Robinson code, proving Theorem 1.1 (a).

Case $(m, \delta) = (15, 5)$: In this case $C(5)$ forms a $2 - (15, 5, 4)$ design, and so $|C(5)| = 42$. Thus, as C is antipodal,

$$a(C) = (1, 0, 0, 0, 0, 42, a_6, a_7, a_7, a_6, 42, 0, 0, 0, 0, 1)$$

By following a similar argument as above, we generate certain inequalities that solve to give $a_6 = 70$ and $a_7 = 15$, and so C is a $(15, 256, 5)$ binary code. Thus, by Snover's result [17], C is equivalent to the punctured Nordstrom-Robinson code, proving Theorem 1.1 (b).

By [12, Lemma 2.6], complete transitivity is preserved by equivalence, and by Theorem 3.2 and Theorem 3.4, the Nordstrom-Robinson codes are completely transitive. Consequently, in both cases, C is completely transitive.

REFERENCES

- [1] Aoki, T., Gaborit, P., Harada, M., Ozeki, M., Solé, P.: On the covering radius of Z_4 -codes and their lattices. *IEEE Trans. Inform. Theory* **45**(6), 2162–2168 (1999). DOI 10.1109/18.782168
- [2] Berlekamp, E.R.: Coding theory and the Mathieu groups. *Information and Control* **18**, 40–64 (1971)
- [3] Borges, J., Rifa, J., Zinoviev, V.A.: On non-antipodal binary completely regular codes. *Discrete Math.* **308**(16), 3508–3525 (2008). DOI 10.1016/j.disc.2007.07.008
- [4] Brouwer, A.E.: A note on completely regular codes. *Discrete Math.* **83**(1), 115–117 (1990). DOI 10.1016/0012-365X(90)90225-7
- [5] Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-regular graphs, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, vol. 18. Springer-Verlag, Berlin (1989)
- [6] Cameron, P.J.: Permutation groups, *London Mathematical Society Student Texts*, vol. 45. Cambridge University Press, Cambridge (1999). DOI 10.1017/CBO9780511623677
- [7] Cameron, P.J., van Lint, J.H.: Designs, graphs, codes and their links, *London Mathematical Society Student Texts*, vol. 22. Cambridge University Press, Cambridge (1991). DOI 10.1017/CBO9780511623714
- [8] Colbourn, C.J., Dinitz, J.H. (eds.): The CRC handbook of combinatorial designs. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL (1996). DOI 10.1201/9781420049954
- [9] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: Atlas of finite groups. Oxford University Press, Eynsham (1985). Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray
- [10] Conway, J.H., Sloane, N.J.A.: Orbit and coset analysis of the Golay and related codes. *IEEE Trans. Inform. Theory* **36**(5), 1038–1050 (1990). DOI 10.1109/18.57203
- [11] Gillespie, N.I., Praeger, C.E.: Uniqueness of certain completely regular Hadamard codes (2011). arXiv:1112.1247v2
- [12] Gillespie, N.I., Praeger, C.E.: From neighbour transitive codes to frequency permutation arrays (2012). arXiv:1204.2900v1
- [13] Giudici, M., Praeger, C.E.: Completely transitive codes in Hamming graphs. *European J. Combin.* **20**(7), 647–661 (1999). DOI 10.1006/eujc.1999.0313
- [14] Goethals, J.M.: On the Golay perfect binary code. *J. Combinatorial Theory Ser. A* **11**, 178–186 (1971)
- [15] van Lint, J.H.: Introduction to coding theory, *Graduate Texts in Mathematics*, vol. 86, third edn. Springer-Verlag, Berlin (1999)
- [16] MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland Publishing Co., Amsterdam (1977). North-Holland Mathematical Library, Vol. 16
- [17] Snover, S.L.: The uniqueness of the Nordstrom-Robinson and the Golay binary codes. ProQuest LLC, Ann Arbor, MI (1973). Thesis (Ph.D.)—Michigan State University
- [18] van Tilborg, H.C.A.: Uniformly packed codes. Technische Hogeschool Eindhoven, Eindhoven (1976). With a Dutch summary, Doctoral dissertation, University of Technology Eindhoven

[GILLESPIE AND PRAEGER] THE CENTRE FOR THE MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, 35 STIRLING HIGHWAY, CRAWLEY, WESTERN AUSTRALIA 6009

E-mail address: `neil.gillespie@graduate.uwa.edu.au`, `cheryl.praeger@uwa.edu.au`